REMARKS

By this Amendment, claims 31-91 are now pending, with claims 1-30 cancelled, and with claims 31-91 added. No new matter is introduced (see, e.g., Specification, as published, paragraphs [0032], [0035]-[0038], [0040], and [0043]-[0050], and FIGs. 1-6). Reconsideration in view of the above amendments and following remarks is respectfully requested.

First, Applicants wish to thank Examiner Popham and his SPE for extending the courtesy of a personal interview with Applicants' undersigned attorney on August 11, 2005. Although no agreement was reached, the new claims, as substantially presented herewith, were discussed and distinguish over the applied references, *Bernhard et al.* (USP 6,275,942), *Joyce* (USP 6,519,703), *Rowland* (USP 6,405,318), and *Cheng et al.* (USP 6,738,909).

Specifically, during the interview, the new independent claims, as substantially presented herewith, were argued to distinguish over the applied references, as being directed to a novel arrangement of a system and method for protecting a distributed network from unauthorized access, including an intrusion detection system, having an intrusion detection module, and a communications management module coupled to the intrusion detection module, and intrusion analysis system coupled to the intrusion detection system, and having an intrusion analysis module, and an intrusion reaction coordination module coupled to the intrusion analysis module in the manner claimed. However, although the applied references may be directed to various components within the claimed arrangement, the applied references fail to disclose, teach or suggest the novel arrangement and features thereof in the manner claimed.

For example, *Bernhard et al.* is directed to system, method and computer program product for automatic response to computer system misuse using active response modules (ARMs) that are tools that allow static intrusion detection system applications the ability to dynamically increase security levels by allowing real-time responses to detected instances of computer misuse and, once defined, are deployed in a "plug and play" manner into an existing intrusion detection system within a computing environment, and upon receipt of an instance of the computer misuse from the intrusion detection system, each ARM linked to the misuse collects pertinent data from the intrusion detection system and invokes a response specified by the ARM class and the collected pertinent data. However, *Bernhard et al.* fails

disclose, teach or suggest the novel arrangement and features thereof in the manner recited in new independent claims 1 and 61.

Joyce is directed to method for processing packets in a computer communication network that includes steps of analyzing a packet stream using at least a first heuristic stage trained to recognize potentially harmful packets, assigning a confidence rating to packets in the analyzed stream in accordance with a level of confidence regarding the harmfulness of the analyzed packets, and selecting packets for further analysis in accordance with their assigned confidence rating. However, *Joyce* fails to disclose, teach or suggest the novel arrangement and features thereof in the manner recited in new independent claims 1 and 61.

Rowland is directed to a computer-implemented intrusion detection system and method that monitors a computer system in real-time for activity indicative of attempted or actual access by unauthorized persons or computers, wherein the system detects unauthorized users attempting to enter into a computer system by comparing user behavior to a user profile, detects events that indicate an unauthorized entry into the computer system, notifies a control function about the unauthorized users and events that indicate unauthorized entry into the computer system and has a control function that automatically takes action in response to the event. However, *Rowland* fails to disclose, teach or suggest the novel arrangement and features thereof in the manner recited in new independent claims 1 and 61.

Cheng et al. is directed to method and apparatus for use in data processing system for selecting rules to filter data for a tunnel, wherein a request is received to create a tunnel to another data processing system, a granularity of information about the data processing system is identified to form an identified granularity, the identified granularity of the information about the data processing system is used to select a rule, which matches the identified granularity, the rule is placed in a filter, and the filter associates data packets with the tunnel. However, *Cheng et al.* fails to disclose, teach or suggest the novel arrangement and features thereof in the manner recited in new independent claims 1 and 61.

Moreover, new independent claims 1 and 61 distinguish over the applied references, taken alone or in combination. The dependent claims are allowable over the applied references, taken alone or in combination, on their on merits, and for at least the reasons advanced with respect to independent claims 31 and 61.

In view of the foregoing, it is submitted that the present application is in condition for allowance and a notice to that effect is respectfully requested. If, however, the Examiner deems that any issues remain after considering this response, the Examiner is invited to contact the undersigned attorney to expedite the prosecution and engage in a joint effort to work out a mutually satisfactory solution.

Respectfully submitted,

NIXON PEABODY, LLP

Carlos R. Villamar
Reg. No. 43,224

Customer No. 22204
NIXON PEABODY LLP
401 9th Street, N.W., Suite 900
Washington, DC 20004
Tel: 202-585-8000
Fax: 202-585-8080